

NEW CLAIM:

New claim 16 has been added to further emphasize that the present invention provides a cipher designing method for designing cipher logic of a cipher device using an F-function to convert input bits to output bits via S-boxes including "generating a plurality of S-boxes each having an input and an output bit number selected based on memory capacity of a memory provided to the cipher device".

As also recited in new claim 16, "the input and output bit number are selected by extracting a set of input and output numbers of the S-boxes based on an entire input and output bit number of a block and determining a combination set based on the memory capacity provided to the cipher device". This allows the present invention to provide cipher logics that enable full utilization of memory, which is read out in one cycle, thereby enhancing processing speed.

Accordingly, newly added claim 16 is patentably distinguishable from the cited references.

CONCLUSION:

In accordance with the foregoing, new claim 16 have been amended. Thus, claims 1-16 are pending and under consideration.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 7/22/4

By: J. Randall Beckers

J. Randall Beckers

Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501